Claims:

1. (PREVIOUSLY PRESENTED) A public-key encryption process comprising the steps of:

   a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message; and

   b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step.

2. (ORIGINAL) A public-key encryption process according to claim 1, wherein the encrypting step uses an El Gamal encryption scheme.

3. (PREVIOUSLY PRESENTED) A public-key encryption process according to claim 1, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme;

   wherein the step of generating the digital signature includes hashing the plaintext message.

4. (ORIGINAL) A public-key encryption process according to claim 1, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$, where G is a generator.

5. (ORIGINAL) A public-key encryption process according to claim 1, for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key $A = aG$, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A.

6. (ORIGINAL) A public-key encryption process according to claim 5, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$.

7. (ORIGINAL) A public-key encryption process according to claim 6, further comprising the steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message.

8. (ORIGINAL) A public-key encryption process according to claim 7, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral

public key to generate a digital signature.

9. (ORIGINAL) A public-key encryption process according to claim 8, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver.

10. (ORIGINAL) A public-key encryption process according to claim 9, further comprising the steps of, at the receiver, generating the secret key $K = bX = bxG = xbG = xB$, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s.

11. (PREVIOUSLY PRESENTED) A public-key encryption process according to claim 1, implemented in a wireless communication system;

wherein at least a two stage public-key encryption process is used;

wherein the first stage includes key establishment and the second stage includes encryption/decryption;

wherein said steps (a) and (b) are performed during the second stage of encryption.

12. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a wireless hand-held communication device.

13. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a personal digital assistant.

14. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a cellular phone.

15. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a two-way pager.

16. (PREVIOUSLY PRESENTED) A public-key encryption system comprising:

a) means for encrypting a plaintext message into a ciphertext message, the means for encrypting producing an ephemeral key pair that is used to encrypt the plaintext message; and

b) means for generating a digital signature using the ephemeral key pair produced by the encrypting means.

17. (ORIGINAL) A public-key encryption system according to claim 16, wherein the means for encrypting employs an El Gamal encryption scheme.

18. (PREVIOUSLY PRESENTED) A public-key encryption system according to claim 16, wherein the means for generating a digital signature generates the digital signature using a Nyberg-Rueppel digital signature scheme.

19. (ORIGINAL) A public-key encryption system according to claim 16, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$ where G is a generator.

20. (ORIGINAL) A public-key encryption system according to claim 16, for encrypting messages for communication between a sender and a receiver, the system further comprising, at the sender,

a) means for generating a sender private key a; and

b) means for calculating a sender public key $A = aG$, where G is a generator, and at the receiver,

a) means for generating a receiver private key b; and

b) means for calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains authentic copy of the sender public key A.

21. (ORIGINAL) A public-key encryption system according to claim 20, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$.

22. (ORIGINAL) A public-key encryption system according to claim 21, wherein the means for encrypting generates a secret key $K = xB$ and uses the secret key K to encrypt a

plaintext message and thereby generate a ciphertext message.

23. (PREVIOUSLY PRESENTED) A public-key encryption system according to claim 22, wherein the means for generating uses the encryption private key x as a signature ephemeral private key and uses the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

24. (ORIGINAL) A public-key encryption system according to claim 23, wherein the digital signature comprises a first value r and a second value s, the system further comprising, at the sender, means for transmitting the encryption ephemeral public key X, the ciphertext message and only the second value s of the digital signature to the receiver.

25. (ORIGINAL) A public-key encryption system according to claim 24, further comprising, at the receiver, means for decrypting a ciphertext message and means for validating a digital signature, wherein the means for decrypting generates the secret key $K = bX$ and decrypts the transmitted ciphertext message using the generated secret key K, and the means for validating calculates the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validates the digital signature based on the calculated first value r and the transmitted second value s.

26. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a wireless communication system.

27. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a wireless hand-held communication device.

28. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a personal digital assistant.

29. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a cellular phone.

30. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a two-way pager.

31. (PREVIOUSLY PRESENTED) A software program on a computer-readable storage medium, which when executed by a processor performs a public-key encryption process comprising the steps of:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message; and

b) generating a digital signature for the ciphertext message using the ephemeral key.

32. (ORIGINAL) A software program according to claim 31, wherein the encrypting step uses an El Gamal encryption scheme.

33. (PREVIOUSLY PRESENTED) A software program according to claim 31, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme.

34. (ORIGINAL) A software program according to claim 31, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$, where G is a generator.

35. (ORIGINAL) A software program according to claim 31, for encrypting messages for communication between a sender and a receiver, the software program performing the further steps of, at the sender,

a) generating a sender private key a; and

b) calculating a sender public key $A = aG$, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A.

36. (ORIGINAL) A software program according to claim 35, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$.

37. (ORIGINAL) A software program according to claim 36, wherein the software program performs the further steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message.

38. (ORIGINAL) A software program according to claim 37, wherein the software program performs the further steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

39. (ORIGINAL) A software program according to claim 38, wherein the digital signature comprises a first value r and a second value s, the software program performing the further step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver.

40. (ORIGINAL) A software program according to claim 39, the software program performing the steps of, at the receiver, generating the secret key $K = bX = bxG = xbG = xB$, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based

on the calculated first value r and the transmitted second value s.

41. (ORIGINAL) A software program according to claim 31, installed in a wireless communication system.

42. (ORIGINAL) A software program according to claim 31, installed in a wireless hand-held communication device.

43. (ORIGINAL) A software program according to claim 31, installed in a personal digital assistant.

44. (ORIGINAL) A software program according to claim 31, installed in a cellular phone.

45. (ORIGINAL) A software program according to claim 31, installed in a two-way pager.